IB/2004/050147

Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. **Patent application No.** **Demande de brevet n°**

04100167.8 ✓

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Europäisches Patentamt | European Patent Office | Office européen des brevets

Anmeldung Nr:
Application no.: 04100167.8 ✓
Demande no:

Anmeldetag:
Date of filing: 20.01.04 ✓
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method of controlling access to a communication network

In Anspruch genommene Prioriät(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Method of controlling access to a communication network

FIELD OF THE INVENTION

The present invention relates to methods of controlling access to communication networks in situations where users of devices capable of being connected to the networks are potentially unaware of their devices coupling to sources of data in the networks; in particular, but not exclusively, the present invention relates to a method of controlling access to the Internet depending upon choice of data carrier. Moreover, the invention also relates to apparatus operable to function according to the method; for example, the invention is pertinent to apparatus which do not include software browsers for accessing communication networks such as the Internet and yet are arranged to execute user software, for example one or more Java applications, which is capable of accessing these communication networks without users of the apparatus being potentially aware of such access being made.

BACKGROUND TO THE INVENTION

The Internet and similar contemporary data communication networks enable users to access a wide range of subject matter from data servers of the networks arranged to supply data content. Such users conventionally employ browser software applications executing on computer hardware, for example lap-top computers, coupled to the networks for accessing information at the servers. It is known that these browser applications are susceptible to being configured on the computer hardware to access only certain categories of data content provided by the aforesaid servers. For example, the browser applications can be arranged to exclude certain classes of web-sites on the Internet, for example to avoid accessing sites susceptible to providing data content degraded by viruses or to supplying subject matter conventionally regarded to be in aesthetically bad taste.

It is known to control access to electronic content over a network. For example, in a European patent application no. EP 1, 267, 243, there is described a method of transferring information from a data content supplier to a remote location. The content supplier includes one or more databases for supplying data content such as executable software programs (software applications), audio such as MP3 files, still images and pictures, data files, video and any combination of such types of data content. A user is located at the remote location and makes use of an authorizing hybrid optical disc having a ROM portion and a RAM portion. The ROM portion includes a pre-formed identification signature impressed thereinto which is difficult for a pirate to copy. The RAM portion is arranged to include user-specific encrypted information which personalizes the optical disc for that specific user. Moreover, the encrypted information in combination with the ROM identification signature provides a user-personalized secure signature. A content supplier authenticating the user using the user-personalized secure signature is able to determine whether or not the user is authorised to download selected information from the content supplier to memory at the remote location for use by the user. The aforesaid patent application is therefore directed to a problem of determining user access to data content stored in one or more databases, for example in return for payment and/or granted user access rights to the data content.

The inventor has appreciated that a rather different problem to those described in the foregoing can arise with regard to remote computing devices, for example media players, having included thereon computing capacity as well as data storage capacity for storing local data content. Such remote computing devices are arranged to execute one or more software applications susceptible to accessing data content stored locally in the devices and/or accessing data content stored remotely from the devices at one or more databases of a communication network, for example the Internet; these software applications are distinct from conventional browser software applications. For example, with regard to future DVD players and similar dedicated data content presenting devices couplable to communication networks such as the Internet envisaged by the inventor, there will often be no explicit browser software included on the devices; the devices conveniently include a Java Virtual Machine for supporting Java software applications. Such Java applications can invoke communication software, for example Application Program Interfaces (API's) such as Internet access API's, for using network features supported by the Java Virtual Machine. On account of there being no explicit browser application software included in the contemporary DVD players, software applications executing on the DVD players are capable of accessing network data sites without the users being aware.

Thus, the inventor has perceived that the remote computing devices are capable of downloading unsuitable or potentially damaging data content without their users either being aware that such downloading is occurring or being able to hinder such downloading from occurring. In this respect, it is a contemporary trend to arrange for software applications executing on portable computing devices, for example mobile telephones and portable media players such as DVD-players, to exhibit seamless operation to their users when accessing different classes of data content from several sources. As a further problem, the inventor has appreciated that it is potentially feasible for certain undesirable software applications to be downloaded without the users being aware, the undesirable applications enabling third parties to monitor users' activities and hence encroach upon their privacy. Thus, the inventor has appreciated greater control of the selection of downloaded data content is desirable whilst also endeavouring to achieve a seamless-type operation to which users are contemporarily accustomed.

A further problem arises in that communication network databases, for example Internet web-sites, are not necessarily stable with time and can be subject to upgrades and updates; such upgrades and updates can arise without users being aware of them having been implemented. The inventor has appreciated that is beneficial to have an opportunity to avoid web-sites whose updated software is susceptible to causing the user's device to malfunction on account of incompatibility.

SUMMARY OF THE INVENTION

An object of the invention is to provide a method of providing users of computing devices with greater control of data content downloaded from one or more databases remote from the users and/or their devices.

According to a first aspect of the present invention, there is provided a method of controlling access to a communication network, characterized in that the method includes the steps of:

(a) providing a device couplable in communication with the network, the device being arranged to include computing means coupling to associated local data storing means;

(b) arranging for the computing means to execute one or more software applications therein which are at least in part operable to access data content from one or more of the local storing means and the network in a substantially seamless manner to a user of the device;

(c) arranging for the computing means to be at least partially restricted regarding data content that it is capable of receiving from the network and/or requesting from the network.

The invention is of advantage in that it is capable of restricting an extent to which software applications are unintentionally loadable into the computing means when such applications are capable of having access to data available within the device.

Preferably, in the method, the device is arranged to function to communicate with the network by software means other than one or more browser software applications. Use of software means other than a browser is beneficial in certain classes of products, for example dedicated media players such as DVD-players, where seamless product operation is to be presented to users of the products without the users being aware of the products accessing data sources remote from the products by way of a browser.

Preferably, in the method, the device is capable of being restricted according to one or more of the following categories:-

(d) access/no-access to the network;

(e) access to the network subject to user authorisation;

(f) access to the network as defined by in a parameter list maintained in association with the device; and

(g) access to the network as defined in association with a given data carrier compatible with the storing means.

These categories are of benefit in that they address principal categories of access which are likely to be of concern to the user.

Preferably, in the method, in step (e), the user is presented with a choice of whether or not to authorise on at least a first occasion a new given data content delivering site in the network is to be accessed. Such an approach allows for subsequent apparent substantially seamless execution of software applications in the device but nevertheless provides the user with a high degree of initial control of choice of sources of data content usable by the device.

Preferably, in the method, the user is presented with one or more Uniform Resource Locators (URL) to authorise for the device to access. Such definition of access to a specific URL allows the user to avoid known problem web-sites which are known by way of the URL's.

Preferably, in the method, device is settable to be subject to a default degree of access to the network which is susceptible to being overridden by at least one of:

(h) user's choice; and

(i) degree of access determined in association with a given data carrier presented to the storing means.

Preferably, in the method, the device is operable to return to a default state of access to the network when one or more of re-booted or powered down.

Preferably, in the method, wherein the partial restriction applied to the computing means in step (c) is arranged to at least partially hinder software applications being downloaded from the network to the device which are executable on the computing means to enable access to data content present in the device from the network.

Preferably, in the method, the degree of access to the network is dependent upon one or more data carriers presented to the storing means. Thus, each data carrier inserted by the user into the device can each have associated therewith a correspondingly defined degree of access. Such linking of degree of access to particular data carrier is of advantage in that it circumvents a need for the user to have to manually reconfigure the device explicitly for each data carrier used with the device. Alternatively, or additionally, the degree of access can be determined by particular parameters carried on one or more data carriers, for example in response to a keyword such as "Disney" signifying a particular category of programme data content.

Preferably, the network corresponds to the Internet and the device is a portable handheld apparatus, more preferably an optical disc data medium player or a DVD-player.

Preferably, in the method, the storing means is arranged to accept one or more optical memory discs, electronic memory modules and magnetic discs as data carriers to provide executable software applications and/or data content to the computing means.

According to a second aspect of the present invention, there is provided a device for communicating with a communication network, characterized in that the device is arranged to include computing means coupling to associated local data storing means, the computing means being operable to execute one or more software applications therein which are at least in part capable of accessing data content from one or more of the local storing means and the network in a substantially seamless manner to a user of the device, and the computing means is arranged to be at least partially restricted regarding data content that it is capable of receiving from the network and/or requesting from the network.

It will be appreciate that features of the invention are susceptible to being combined in any combination without departing from the scope of the invention.

DESCRIPTION OF THE DIAGRAMS

Embodiments of the invention will now be described, by way of example only, with reference to the following diagrams wherein:

Figure 1 is an illustration of a communication network including a remote terminal; and

Figure 2 is an illustration of the terminal arranged to accept data carriers for providing data content and/or software to the terminal.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

In overview with regard to the present invention, the inventor has envisaged that a computer-based product including a computing device coupled to an associated memory device and also to a communication interface for connecting the product in communication with one or more database situated remotely from the product is preferably provided with a feature, implemented in hardware and/or software, which controls a degree to which a user of the product has access to the one or more databases, for example one or more servers coupled to the Internet; for example, the product is preferably a DVD player including a Java Virtual Machine capable of executing software stored on a DVD data carrier provided to the player, the data carrier including executable software applications and/or data content. The computing device is arranged to be configurable by way of a set of configuration parameters to exhibit in operation various degrees of acceptance of categories of data content received at the product from the one or more databases and/or sent as requests for data content from the product to the one or more data bases. These configuration parameters are beneficially selectable for different software applications which can be executed on the computing device; for example, a first given software application can be authorised by a user of the device to access and/or receive data from the one or more databases whereas a second given software application can be authorised to have no access to the one or more databases. Intermediate degrees of access to the one or more databases and/or limited categories of data accepted from the one or more databases are also selectable by the user for each software application. More preferably, the software applications are introduced into the product by inserting one or more data carriers into the product. Additionally, or alternatively, one or more of the software applications are susceptible to being downloaded from the one or more databases. The aforesaid configuration parameters are beneficially settable for each of the data carriers; for example, each DVD data carrier useable with the product can have an associated set of configuration parameters which control a degree to which software applications included on the data carrier are capable, when executed within the product, of accessing data stored on databases remote from the product and/or included on the data carrier. For example, the user inserting a given data carrier, for example a proprietary "Blu-ray" optical disc data carrier as developed by Philips Corporation, into the product will invoke an associated set of configuration parameters for that data carrier determining an extent to which software applications recorded on the data carrier can access data content on the one or more databases. Thus, one data carrier can be arranged so that its software applications have Internet access whereas another data carrier can be arranged so that its software applications are denied access to the Internet. The data parameters can be stored in other memory included in the product, for example in non-volatile memory associated with the computing device of the product. Moreover, the configuration parameters can be at least one of user selectable and vendor selectable.

In order to further elucidate the present invention, an embodiment thereof will now be described with reference to Figure 1.

In Figure 1, there is a communication network indicated generally by 10. The network 10 includes a remote terminal 20 coupled by way of a communication link 30 to a network infrastructure 40 including one or more servers, for example a server 50, operable to provide one or more accessible databases. The communication link 30 is one or more of a wireless link, a wire link and an optical link; the wireless link is preferably implemented in a manner akin to a mobile telephone and/or proprietary Blue-Tooth. The remote terminal 20 is preferably implemented as a data medium player, for example a DVD player.

The terminal 20 includes a computer processor (CPU) 60 coupled to a local memory device 70 and a user interface 80. The processor (CPU) 60 is preferably operable to provide a Java Virtual Machine for executing one or more Java software applications. Moreover, the user interface 80 is operable to interact with a user 90 of the terminal 20. Moreover, the user interface 80 comprises at least one of:

(a) a visual interface for presenting an image to the user 90, for example a pixel liquid crystal display (LCD);

(b) a visual sensor for visually monitoring the user 90, for example a miniature digital camera;

(c) an acoustic sensor for recording sound in environs of the user 90, for example a microphone;

(d) an acoustic transducer for generating acoustic sound for the user 90, for example a diaphragm loudspeaker or a piezo-electric (PZT) sound generating element; and

(e) one or more control switches and/or sensors susceptible to being actuated by the user 90 to input data into the terminal 20, for example an array of push-buttons.

The local memory device 70 is one or more of a magnetic hard disc drive (HDD) memory and an optical disc memory; more preferably, the disc memory is a proprietary "Blu-ray" disc drive devised by Philips Corporation in the Netherlands. Beneficially, the memory device 70 is capable of receiving removable data carriers such as proprietary "Blu-ray" ROMs. Additionally, or alternatively, the memory device 70 includes non-volatile solid-state memory, for example a data cache for short-term data buffering.

In a first preferred embodiment, the terminal 20 is arranged to be a "Play-Station" on which the user 90 can play games. Children are susceptible to using the terminal 20 and it is therefore desirable to prevent them from accessing certain categories of Internet data content, for example violent scenes and erotic scenes.

In a second preferred embodiment, the terminal 20 is a portable hand-held shopping device to assist the user 90 select goods for purchase. It is desirable to prevent software applications from loading from the one or more servers 50 which can execute of the processor 60 to download purchase choices made by the user 90 and thereby violate the user's 90 privacy.

In a third preferred embodiment, the terminal 20 is an emergency assistance device employed by paramedics when attending accident scenes. The aforementioned visual sensor of the interface 80 can be used to send images of a crash scene to a remote locality, for example to a hospital, for independent assessment and preparation thereat for receiving crash victims; where horrific or embarrassing images of a crash victim's body are communicated through the terminal 20 to the infrastructure 40, it is desirable that third party software applications are not inadvertently downloaded to the terminal 20 communicating such horrific or embarrassing images to a third party, for example a newspaper, which subsequently in an unauthorised manner divulges such images to the public.

In a fourth preferred embodiment, the terminal 20 is a portable DVD-player capable of receiving DVD data carriers, for example implemented in contemporary "Blu-Ray"-type optical disc format.

Operation of the network 10 will now be described with reference to Figure 1.

The computer processor 60 executes operating system (OS) software which enables it to create an environment within the terminal 20 in which one or more software applications, for example applications including Internet access APIs, are capable of executing; the operating system is preferably stored in user inaccessible ROM incorporated at manufacture into the terminal 20; more preferably, the operating system (OS) is implemented to include a Java Virtual Machine capable of executing Java software applications including

Internet APIs. Amongst other features, the operating system (OS) is operable to load software applications from one or more data carriers inserted into the memory device 70 to run on the processor 60. The loaded software applications communicate to the user 90 via the interface 80 and also access data content stored in the inserted data carriers. As elucidated in the foregoing, the loaded software applications are also susceptible to communicate via the communication link 30 to the one or more servers 50 to access at least one of data and executable software applications, for example software API's, therefrom. Such data and/or executable software applications are then loaded via the communication link 30 to random access memory (RAM) of the processor 60; in the case of executable software applications, they are executed by the processor 60 to affect presentation of subject matter to the user 90.

Software applications executing on the processor 60 are preferably arranged to be "seamless" to the user 90 in respect of whether they are accessing data from the local memory device 70 or data from the infrastructure 40. Such seamless operation is to be distinguished from a contemporary personal computer (PC) where a user thereof explicitly invokes browser software applications for purposes of accessing the Internet or similar data communication networks and the user is therefore aware of when the user's computer is downloading data content; such an aspect fundamentally distinguishes the present invention from conventional computers arranged to execute explicitly invoked browser software applications for accessing communication networks such as the Internet. However, seamless operation of the terminal 20 is also problematical in that rogue software applications can also potentially be unintentionally downloaded from the infrastructure 40 and/or from the memory device 70 and run concurrently in the terminal 20 accessing data content stored in the memory device 70 or downloading images and/or sounds recorded by the interface 80 and passing these via the communication link 30 to the infrastructure 40 where it can be accessed by third parties, thereby violating user privacy. Where data content stored on the memory device 70 pertains to private information, such rogue software applications are also susceptible to violating user privacy by accessing such private information.

In addition to privacy issues, selectively preventing Internet access from the terminal 20 is desirable where Internet access is charged to the user 90 on a byte-basis when the user 90 merely desires to watch a movie on the interface 80, the movie being recorded on a data carrier inserted into the memory device 70.

As elucidated in general overview in the foregoing, the terminal 20 is arranged to employ configuration parameters to control an extent to which software applications executing on the processor 60 are capable of accessing and/or accepting data content from the infrastructure 40, for example from the Internet. Preferably, the configuration parameters are graded to permit the following categories of access:

(A) no access to the infrastructure 40, for example no access to the Internet;

(B) only allow access to the infrastructure 40 (for example the Internet) subject to approval from the user 90, for example by presenting to the user 90 with a visual selection option on the interface 80 to which the user 90 responds by depressing a switch (not shown) on the terminal 20 whether or not to proceed to access the infrastructure 40; optionally, the aforesaid visual selection option includes Uniform Resource Locator (URL) details presented of a site in the infrastructure 40 (for example an Internet web site) for which permission from the user 90 is desired;

(C) only allow access to the infrastructure 40 (for example the Internet) if a site therein to be accessed is recorded in an approved list recorded in the terminal 20; the list is preferably implemented as a list of URL's where the infrastructure 40 corresponds to the Internet; and

(D) access rights associated with one or more of the user's data carriers, for example Blu-ray optical memory disc, insertable into the memory device 70.

The categories of access (A) to (D) are not mutually exclusive, for example the category (B) can be invoked in conjunction with the categories (C) and (D). In particular, the category (C) concerning a list of approved URL's can be all the URL's that the user 90 is permitted to approve for access in the category (B). By using the configuration parameters complying with one or more of the categories (A) to (D), the user 90 can allow access to certain Internet domains, for example movie studio web sites, and not to others, for example advertising and tracking sites.

The aforementioned configuration parameters are user settable. Alternatively, or additionally, the configuration parameters are provided or set at manufacture of the terminal 20. Thus, as shown in Figure 2, a first data carrier 200a capable of being accepted by the memory device 70 is configured for the categories (B), (C) and (D) whereas a second such data carrier 200b is configured for the category (A) only.

The terminal 20 is capable of being arranged to function so that the user 90 can set a default option for the configuration parameters and also to amend the configuration parameters for a current session of use of the terminal 20. Such amended configuration parameters are preferably user settable for each data carrier, for example optical disc ROM, or until the terminal 20 is switched off after a session of use by the user 90.

In one preferred embodiment of the invention, the configuration parameters are selectable from a configuration menu presented on the interface 80 to the user 90, for example in a manner akin to setting a default language in MicroSoft Windows computer environments; "Windows" is a trade mark of MicroSoft Corporation.

The terminal 20 is preferably operable to remember changes to the configuration parameters implemented by the user 90 with regard to a given data carrier, for example optical disc inserted into the memory device 70, for future use when the given data carrier is subsequently reinserted into the terminal 20.

In the category (C) above, the user 90 is preferable permitted to add URL's to the list either by way of confirmation of URL options presented on the interface 80, for example by way of a subsidiary list of optionally invocable URL's, or by way of the user 90 inputting URL details, for example by way of an alpha-numeric keypad in a similar manner to which SMS messages are contemporarily entered on mobile telephones.

It will be appreciated that embodiments of the invention described in the foregoing are susceptible to being modified without departing from the scope of the invention.

In the foregoing, and also with regard to the appended claims, expressions such as "include", "comprise", "contain", "incorporate", "have" and "is" are to be construed non-exclusively, namely allowing for one or more items or components not explicitly disclosed also to be present. Reference to the singular is also to be construed as referring to the plural and vice versa.

CLAIMS:

1. A method of controlling access to a communication network (40, 50), characterized in that the method includes the steps of:

(a) providing a device (20) couplable in communication with the network (40, 50), the device (20) being arranged to include computing means (60) coupling to associated local data storing means (70, 200a, 200b);

(b) arranging for the computing means (60) to execute one or more software applications therein which are at least in part operable to access data content from one or more of the local storing means (70, 200a, 200b) and the network (40, 50) in a substantially seamless manner to a user (90) of the device (20);

(c) arranging for the computing means (60) to be at least partially restricted regarding data content that it is capable of receiving from the network (40, 50) and/or requesting from the network (40, 50).

2. A method according to Claim 1, wherein the device (20) is arranged to function to communicate with the network (40, 50) by software means other than one or more browser software applications.

3. A method according to Claim 1, wherein the device (20) is capable of being restricted according to one or more of the following categories:-

(d) access/no-access to the network (40, 50);

(e) access to the network (40, 50) subject to user (90) authorisation;

(f) access to the network (40, 50) as defined by in a parameter list maintained in association with the device (20); and

(g) access to the network (40, 50) as defined in association with a given data carrier (200a, 200b) compatible with the storing means (70).

4. A method according to Claim 3, wherein in step (e) the user (90) is presented with a choice of whether or not to authorise on at least a first occasion a new given data content delivering site (50) in the network (40, 50) is to be accessed.

5. A method according to Claim 4, wherein the user (90) is presented with one or more Uniform Resource Locators (URL) to authorise for the device (20) to access.

6. A method according to Claim 1, wherein the device (20) is settable to be subject to a default degree of access to the network (40, 50) which is susceptible to being overridden by at least one of:

(h) user's (90) choice; and

(i) degree of access determined in association with a given data carrier presented to the storing means.

7. A method according to Claim 6, wherein the device (20) is operable to return to a default state of access to the network (40, 50) when one or more of re-booted or powered down.

8. A method according to Claim 1, wherein the degree of access to the network (40, 50) is dependent upon one or more data carriers presented to the storing means.

9. A method according to Claim 1, wherein the partial restriction applied to the computing means (60) in step (c) is arranged to at least partially hinder software applications being downloaded from the network (40, 50) to the device (20) which are executable on the computing means (60) to enable access to data content present in the device (20) from the network (40, 50).

10. A method according to Claim 1, wherein the network (40, 50) corresponds to the Internet and the device (20) is a portable handheld apparatus, more preferably an optical disc data medium player or a DVD-player.

11. A method according to Claim 1, wherein the storing means (70) is arranged to accept one or more optical memory discs, electronic memory modules and magnetic discs as data carriers to provide executable software applications and/or data content to the computing means (60).

12. A device (20) for communicating with a communication network (40, 50), characterized in that the device (20) is arranged to include computing means (60) coupling to associated local data storing means (70, 200a, 200b), the computing means (60) being operable to execute one or more software applications therein which are at least in part capable of accessing data content from one or more of the local storing means (70, 200a, 200b) and the network (40, 50) in a substantially seamless manner to a user (90) of the device (20), and the computing means (60) is arranged to be at least partially restricted regarding data content that it is capable of receiving from the network (40, 50) and/or requesting from the network (40, 50).

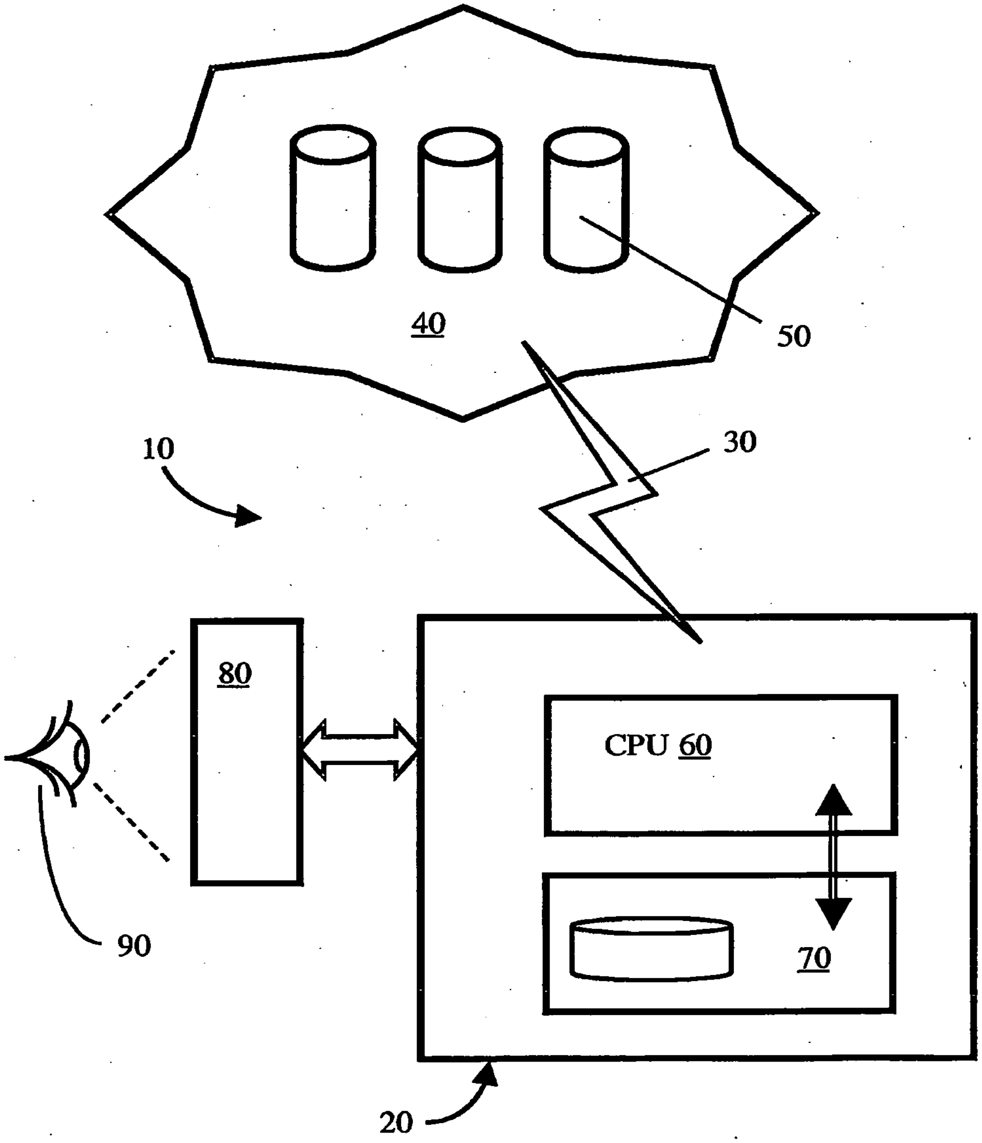

FIG.1

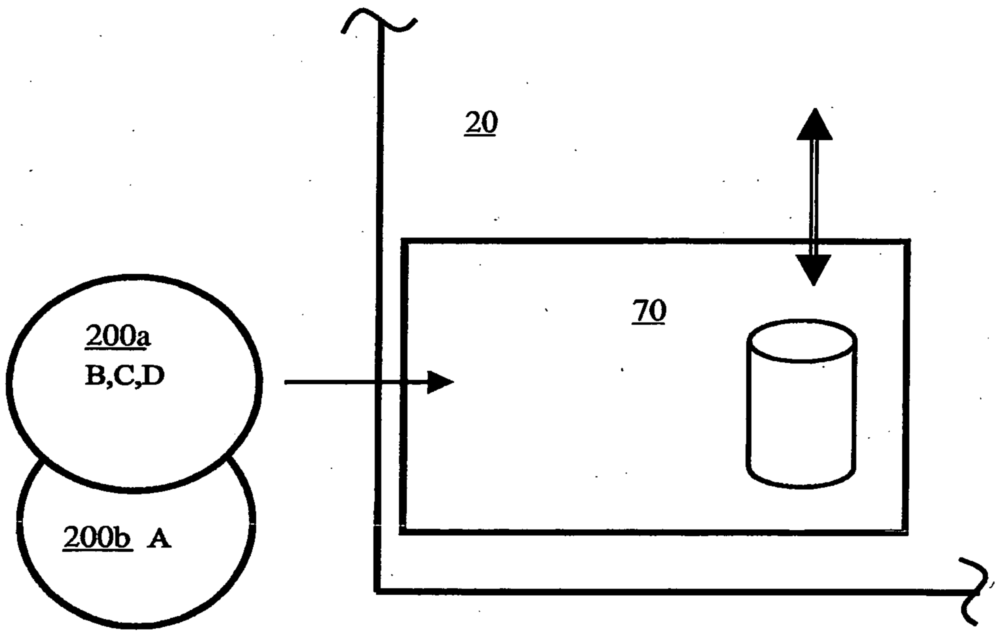

FIG.2